# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-271318
(43)Date of publication of application : 20.09.2002

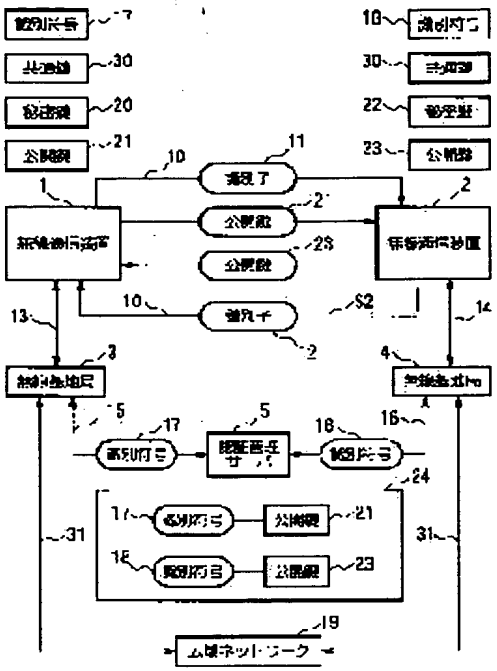
(51)Int.Cl. H04L 9/32
H04L 9/08
H04L 12/28

(21)Application number : 2001-062084
(22)Date of filing : 06.03.2001

(71)Applicant : MITSUBISHI MATERIALS CORP
(72)Inventor : KURAMOTO EITARO

## (54) RADIO COMMUNICATION EQUIPMENT AND CERTIFICATION MANAGING SERVER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide radio communication equipment which can inform an IP address to a communication partner without being known by outsiders.
SOLUTION: Radio communication equipment 1 transmits an identifier 11 to radio communication equipment 2 with a short distance communication part, and receives an identifier 12 of the radio communication equipment 2 therefrom. A common key producing part produces a common key 30 by using the identifier 11 and the received identifier 12. A key producing part produces a disclosure key 21 and a secret key 20 by using an identification code 11 of the radio communication equipment 1 which is issued from a radio base station 3 and the common key 30. A control unit transmits the disclosed key 21 to the radio communication equipment 2 with the short distance communication part. When communication is performed to the communication equipment, the control unit transmits a disclosed key 23 received from the radio communication equipment 2 to a certification managing server 5 as a communication destination, and receives an identification code 17 of the radio communication equipment 2 from the certification managing server 5.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－271318
（P2002－271318A）
(43)公開日　平成14年９月20日(2002.9.20)

| (51)Int.Cl.' | 識別記号 | ＦＩ | テーマコード'(参考) |
|---|---|---|---|
| Ｈ０４Ｌ　9/32 | | Ｈ０４Ｌ　12/28 | ３００Ｚ　５Ｊ１０４ |
| 9/08 | | 9/00 | ６７３Ｂ　５Ｋ０３３ |
| 12/28 | ３００ | | ６０１Ｄ |
| | | | ６０１Ｅ |
| | | | ６０１Ｆ |

審査請求　未請求　請求項の数10　ＯＬ　（全 11 頁）

(21)出願番号　特願2001－62084(P2001－62084)

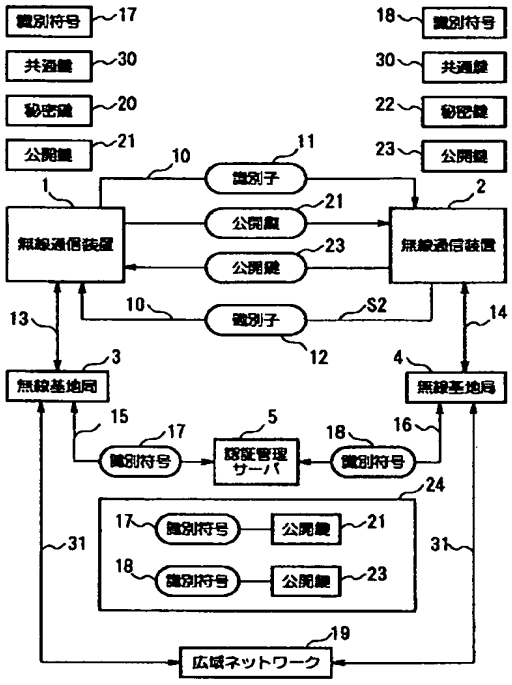
(22)出願日　平成13年３月６日(2001.3.6)

(71)出願人　000006264
三菱マテリアル株式会社
東京都千代田区大手町１丁目５番１号
(72)発明者　倉本　英太郎
東京都文京区小石川一丁目12番14号　三菱マテリアル株式会社移動体事業開発センター内
(74)代理人　100064908
弁理士　志賀　正武　（外６名）

Ｆターム(参考)　5J104 AA03 AA07 AA09 AA16 EA04
EA16 EA26 KA02 LA06 MA01
NA02 PA07
5K033 AA08 CB01 CC01 DA06 DA19
DB04 DB18 EA07 EC01 EC03

(54)【発明の名称】　無線通信装置、認証管理サーバ

(57)【要約】
【課題】　ＩＰアドレスを第３者に知られないように通信相手に通知することができる無線通信装置を提供する。
【解決手段】　無線通信装置１は、近距離通信部によって識別子１１を無線通信装置２に送信し、無線通信装置２の識別子１２を無線通信装置２から受信する。共通鍵生成部は、識別子１１と受信した識別子１２とによって共通鍵３０を生成する。鍵生成部は、無線基地局３から発行される無線通信装置１の識別符号１１と共通鍵３０とによって公開鍵２１と秘密鍵２０を生成する。そして、制御部は、近距離通信部によって公開鍵２１を無線通信装置２に送信する。また、制御部は、無線通信装置に対して通信を行う場合に、無線通信装置２から受信した公開鍵２３を通信先として認証管理サーバ５に送信し、認証管理サーバ５から無線通信装置２の識別符号１７を受信する。



1

【特許請求の範囲】

【請求項１】　少なくとも２経路の通信回線を介して他の無線通信装置に接続される通信システムにおける無線通信装置であって、

第１の通信回線を用いて通信相手となる無線通信装置の登録に関する通信を行う第１の通信手段と、

前記第１の通信手段によって登録された通信相手に対し、前記第１の通信回線と異なる通信回線を用いて通信を行う第２の通信手段と、

を有することを特徴とする無線通信装置。

【請求項２】　前記第１の通信手段は、登録を行う無線通信装置に対して近距離において登録に関する通信を行うことを特徴とする請求項１に記載の無線通信装置。

【請求項３】　少なくとも２経路の通信回線を介して他の無線通信装置に接続される通信システムにおける無線通信装置であって、

自身に設定された識別子を送信するとともに、通信を行う相手側の無線通信装置に設定された識別子を受信する第１の通信手段と、

前記自身に設定される識別子と前記第１の通信手段によって受信する相手側の無線通信装置に設定された識別子とに基づいて、共通鍵を生成する共通鍵生成手段と、

前記共通鍵生成手段によって生成される共通鍵と自身に設定される識別符号とに基づいて公開鍵を生成する公開鍵生成手段と、

前記公開鍵生成手段によって生成される公開鍵を前記第１の通信手段によって前記相手側の無線通信装置に送信するとともに、前記相手側の無線通信装置によって生成された公開鍵を前記相手側の無線通信装置から前記第１の通信手段によって受信して、通信相手として登録する制御手段と、

前記制御手段によって登録された通信相手となる無線通信装置に対し、前記公開鍵生成手段によって生成される公開鍵を用いて前記第１の通信手段とは異なる通信回線を用いて通信を行う第２の通信手段と、

を有することを特徴とする無線通信装置。

【請求項４】　前記第１の通信手段は、近距離において通信を行うことを特徴とする請求項３に記載の無線通信装置。

【請求項５】　少なくとも２台以上の無線通信装置と認証管理サーバとが接続される通信システムにおける認証管理サーバであって、

無線通信装置から送信される固有情報と識別符号との対応関係と、通信相手として信頼関係の確立がなされた無線通信装置同士の対応関係とを認証データとして記憶する記憶手段と、

通信相手となる無線通信装置を指定する固有情報を前記無線通信装置から通信要求として受信した場合、前記受信した固有情報に対応する識別符号を前記記憶手段に記憶された認証データから読み出し、読み出した識別符号を前記通信要求を行った無線通信装置に送信する制御を行う制御手段とを有することを特徴とする認証管理サーバ。

2

【請求項６】　前記制御手段は、信頼関係の確立がなされていない無線通信装置間で通信を行う相手側の無線通信装置の登録を行う場合に、

前記記憶手段に記憶された認証データに基づいて、前記信頼関係の確立がなされていない無線通信装置同士が共通に信頼関係の確立を行っている無線通信装置を介し、通信を行う相手側の無線通信装置の登録を行うように制御することを特徴とする請求項５に記載の認証管理サーバ。

【請求項７】　前記固有情報は、無線通信装置によって生成される公開鍵であることを特徴とする請求項５または請求項６に記載の認証管理サーバ。

【請求項８】　少なくとも２経路の通信回線を介して他の無線通信装置に接続される通信システムにおける無線通信装置における通信相手登録プログラムを記録した記録媒体であって、

前記記録媒体は、

自身に設定された識別子を送信するとともに、通信を行う相手側の無線通信装置に設定された識別子を受信する第１の通信ステップと、

前記自身に設定される識別子と前記受信する識別子とに基づいて共通鍵を生成する共通鍵生成ステップと、

前記共通鍵生成ステップによって生成される共通鍵と自身に設定される識別符号とに基づいて公開鍵を生成する公開鍵生成ステップと、

前記公開鍵生成ステップによって生成される公開鍵を前記第１の通信ステップにおける通信回線を介して前記相手側の無線通信装置に送信する送信ステップと、

前記相手側の無線通信装置によって生成された公開鍵を前記相手側の無線通信装置から前記第１の通信ステップにおける通信回線を用いて受信して、通信相手として登録する登録ステップと、

前記登録ステップによって登録された通信相手となる無線通信装置に対し、前記公開鍵生成ステップによって生成される公開鍵を用いて前記第１の通信ステップにおける通信回線とは異なる通信回線を用いて通信を行う第２の通信ステップと、

をコンピュータに実行させるための通信相手登録プログラムを記録したことを特徴とする記録媒体。

【請求項９】　少なくとも２台以上の無線通信装置と認証管理サーバとが接続される通信システムにおける認証管理サーバにおける通信プログラムを記録した記録媒体であって、

前記記録媒体は、

無線通信装置から送信される固有情報と識別符号との対応関係と、通信相手として信頼関係の確立がなされた無線通信装置同士の対応関係とを認証データとして記憶す

る記憶ステップと、
通信相手となる無線通信装置を指定する固有情報を前記無線通信装置から通信要求として受信した場合、前記記憶ステップにおいて記憶された認証データに基づいて、前記受信した固有情報に対応する識別符号を前記通信要求を行った無線通信装置に送信する制御を行う制御ステップとをコンピュータに実行させる通信プログラムを記録したことを特徴とする記録媒体。

【請求項１０】　少なくとも２経路の通信回線を介して他の無線通信装置に接続される通信システムにおける通信方法であって、
第１の通信回線を用いて通信相手となる無線通信装置の登録に関する通信を行い、前記登録された通信相手に対し、前記第１の通信回線と異なる通信回線を用いて通信を行うことを特徴とする通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、無線によって通信を行う無線通信装置に係り、特に、無線通信装置に設定される識別符号の秘匿性を向上させて通信を行う無線通信装置に関するものである。

【０００２】

【従来の技術】従来から、通信相手となる端末と自身の端末との相互間において、インターネット等のネットワークを介して、データの送受信を行う方法が知られている。通信したい相手に、自身のアドレス（ＩＰアドレス、メールアドレス、電話番号等）を教える場合、例えば、端末の利用者は、通信相手に自分のアドレスを口頭で伝えたり、アドレスを記入したメモを通信相手に渡す等していた。

【０００３】

【発明が解決しようとする課題】しかしながら、従来は、口頭でアドレスを通信相手に教える場合、近くにいる第３者によってアドレスが聞き取られると、アドレスを教えたい相手以外にアドレスが知られてしまう可能性があった。また、従来は、アドレスを記入したメモを相手に渡す場合、メモに書かれたアドレスが、第３者によって見られてしまい、アドレスを教えたい相手以外にアドレスが知られてしまう可能性があった。例えば、上述した状況下において、悪意ある第３者にアドレスが知られてしまうと、この悪意ある第３者からＤｏＳ攻撃を受ける可能性がある。ここで、ＤｏＳ攻撃とは、インターネット経由でサーバやシステムに過負荷をかけてサービス停止に追い込む行為のことをいう。このように、従来においては、アドレスなどの端末固有の識別符号を通信相手に教える場合に、アドレスが第３者に漏洩してしまうという問題点があった。

【０００４】本発明は、このような事情に鑑みてなされたもので、その目的は、識別符号であるＩＰアドレスを第３者に知られないように通信相手に通知することができる無線通信装置を提供することにある。



【０００５】

【課題を解決するための手段】上記目的を達成するために、本発明は、少なくとも２経路の通信回線を介して他の無線通信装置に接続される通信システムにおける無線通信装置であって、第１の通信回線を用いて通信相手となる無線通信装置の登録に関する通信を行う第１の通信手段（例えば、実施の形態における近距離通信部）と、前記第１の通信手段によって登録された通信相手に対し、前記第１の通信回線と異なる通信回線を用いて通信を行う第２の通信手段（例えば、実施の形態における遠距離通信部）とを有することを特徴とする。

【０００６】また、本発明は、上述の無線通信装置において、前記第１の通信手段は、登録を行う無線通信装置に対して近距離において登録に関する通信を行うことを特徴とする。

【０００７】また、本発明は、少なくとも２経路の通信回線を介して他の無線通信装置に接続される通信システムにおける無線通信装置であって、自身に設定された識別子を送信するとともに、通信を行う相手側の無線通信装置に設定された識別子を受信する第１の通信手段と、前記自身に設定される識別子と前記第１の通信手段によって受信する相手側の無線通信装置に設定された識別子とに基づいて、共通鍵を生成する共通鍵生成手段（例えば、実施の形態における共通鍵生成部１５１）と、前記共通鍵生成手段によって生成される共通鍵と自身に設定される識別符号とに基づいて公開鍵を生成する公開鍵生成手段（例えば、実施の形態における鍵生成部）と、前記公開鍵生成手段によって生成される公開鍵を前記第１の通信手段によって前記相手側の無線通信装置に送信するとともに、前記相手側の無線通信装置によって生成された公開鍵を前記相手側の無線通信装置から前記第１の通信手段によって受信して、通信相手として登録する制御手段（例えば、実施の形態における制御部１６０）と、前記制御手段によって登録された通信相手となる無線通信装置に対し、前記公開鍵生成手段によって生成される公開鍵を用いて前記第１の通信手段とは異なる通信回線を用いて通信を行う第２の通信手段とを有することを特徴とする。

【０００８】また、本発明は、上述の無線通信装置において、前記第１の通信手段は、近距離において通信を行うことを特徴とする。

【０００９】また、本発明は、少なくとも２台以上の無線通信装置と認証管理サーバとが接続される通信システムにおける認証管理サーバであって、無線通信装置から送信される固有情報と識別符号との対応関係と、通信相手として信頼関係の確立がなされた無線通信装置同士の対応関係とを認証データとして記憶する記憶手段（例えば、実施の形態における記憶部５－２）と、通信相手となる無線通信装置を指定する固有情報を前記無線通信装

5

置から通信要求として受信した場合、前記受信した固有情報に対応する識別符号を前記記憶手段に記憶された認証データから読み出し、読み出した識別符号を前記通信要求を行った無線通信装置に送信する制御を行う制御手段（例えば、実施の形態における制御部５－３）とを有することを特徴とする。

【００１０】また、本発明は、上述の認証管理サーバにおいて、前記制御手段は、信頼関係の確立がなされていない無線通信装置間で通信を行う相手側の無線通信装置の登録を行う場合に、前記記憶手段に記憶された認証データに基づいて、前記信頼関係の確立がなされていない無線通信装置同士が共通に信頼関係の確立を行っている無線通信装置を介し、通信を行う相手側の無線通信装置の登録を行うように制御することを特徴とする。

【００１１】また、本発明は、上述の認証管理サーバにおいて、前記固有情報は、無線通信装置によって生成される公開鍵であることを特徴とする。

【００１２】また、本発明は、少なくとも２経路の通信回線を介して他の無線通信装置に接続される通信システムにおける無線通信装置における通信相手登録プログラムを記録した記録媒体であって、前記記録媒体は、自身に設定された識別子を送信するとともに、通信を行う相手側の無線通信装置に設定された識別子を受信する第１の通信ステップと、前記自身に設定される識別子と前記受信する識別子とに基づいて共通鍵を生成する共通鍵生成ステップと、前記共通鍵生成ステップによって生成される共通鍵と自身に設定される識別符号とに基づいて公開鍵を生成する公開鍵生成ステップと、前記公開鍵生成ステップによって生成される公開鍵を前記第１の通信ステップにおける通信回線を介して前記相手側の無線通信装置に送信する送信ステップと、前記相手側の無線通信装置によって生成された公開鍵を前記相手側の無線通信装置から前記第１の通信ステップにおける通信回線を用いて受信して、通信相手として登録する登録ステップと、前記登録ステップによって登録された通信相手となる無線通信装置に対し、前記公開鍵生成ステップによって生成される公開鍵を用いて前記第１の通信ステップにおける通信回線とは異なる通信回線を用いて通信を行う第２の通信ステップと、をコンピュータに実行させるための通信相手登録プログラムを記録したことを特徴とする。

【００１３】また、本発明は、少なくとも２台以上の無線通信装置と認証管理サーバとが接続される通信システムにおける認証管理サーバにおける通信プログラムを記録した記録媒体であって、前記記録媒体は、無線通信装置から送信される固有情報と識別符号との対応関係と、通信相手として信頼関係の確立がなされた無線通信装置同士の対応関係とを認証データとして記憶する記憶ステップと、通信相手となる無線通信装置を指定する固有情報を前記無線通信装置から通信要求として受信した場

6

合、前記記憶ステップにおいて記憶された認証データに基づいて、前記受信した固有情報に対応する識別符号を前記通信要求を行った無線通信装置に送信する制御を行う制御ステップとをコンピュータに実行させる通信プログラムを記録したことを特徴とする。

【００１４】また、本発明は、少なくとも２経路の通信回線を介して他の無線通信装置に接続される通信システムにおける通信方法であって、第１の通信回線を用いて通信相手となる無線通信装置の登録に関する通信を行い、前記登録された通信相手に対し、前記第１の通信回線と異なる通信回線を用いて通信を行うことを特徴とする。

【００１５】

【発明の実施の形態】以下、本発明の一実施形態による無線通信装置を図面を参照して説明する。図１は、この発明の一実施形態による無線通信装置、認証サーバを適用した通信システムの構成を示す概略ブロック図である。この図において、無線通信装置１および無線通信装置２は、第１の通信回線または第２の通信回線を介して相互に通信を行う。また、無線通信装置１は、端末１－１～端末１－ｎと通信を行い、無線通信装置２は、端末２－１～端末２－ｍと通信を行う。

【００１６】１０は、無線通信装置１および無線通信装置２とを接続し、無線通信装置に設定された識別符号の伝送する近距離通信回線である。この近距離通信回線１０が、第１の通信回線に対応する。この第１の通信回線としては、例えば、赤外線通信やＢＬＵＥＴＯＯＴＨ（近距離無線通信技術）等の無線あるいは接続ケーブルなどの有線によって無線通信装置間を接続するものである。以下、第１の通信回線を介して行う通信を近距離通信と称する。ここでは、例えば、ＢＬＵＥＴＯＯＴＨが近距離通信回線１０として適用される。

【００１７】無線基地局３および無線基地局４は、広域ネットワーク１９を介して相互通信可能に接続される。ここでは、広域ネットワーク１９を介して行う通信を遠距離通信と称する。また、無線基地局３および無線基地局４は、無線によって無線通信装置１または無線通信装置２に接続されるとともに、必要に応じて無線通信装置に識別符号を動的に割り当てる。

【００１８】認証管理サーバ５は、相互に信頼関係を確立した各無線通信装置間の対応関係を示す認証データを記憶する（詳細は後述する）。また、認証管理サーバ５は、公開鍵と公開鍵の利用者に関する情報に基づいて、申請内容のチェックを行い、認証局の電子署名付公開鍵を発行する。

【００１９】１３、１４は、認証データおよび通信データを伝送する通信回線である。この通信回線１３および通信回線１４は、無線によって無線通信装置と無線基地局を接続する。１５、１６は、相互認証情報を登録、参照するための通信回線である。３１は、広域ネットワー

ク１９と無線基地局３、無線基地局４とを接続する通信回線である。広域ネットワーク１９は、例えば、インターネット等のネットワークである。この広域ネットワーク１９を用いる通信回線が第２の通信回線に対応している。すなわち、無線通信装置１と無線通信装置２との間は、第２の通信回線である広域ネットワーク１９を用いるとともに、通信回線１３、無線基地局３、通信回線３１、無線基地局４、通信回線１４を用いて接続される。

【００２０】次に、無線通信装置１について、図２を用いてさらに詳細に説明する。図２は、無線通信装置１の構成を示す概略ブロック図である。この図に示すように、無線通信装置１の通信部１００は、近距離通信部１１０と遠距離通信部１３０とによって構成され、近距離通信回線１０（ここでは、ＢＬＵＥＴＯＯＴＨ）を用いて通信相手となる無線通信装置の登録に関する通信を行う。

【００２１】近距離通信部１１０は、近距離通信回線１０を介して通信相手となる無線通信装置２と近距離における通信を行う。ここで、近距離における通信とは、近距離通信部１１０が通信可能な領域内であり、例えば、通信を行う相手側の無線通信装置の使用者を視覚によって確認できる距離である。また、近距離通信部１１０は、ＢＬＵＥＴＯＯＴＨによって端末１－１～端末１－ｎと通信を行う。なお、近距離通信部１１０と端末１－１～端末１－ｎは、赤外線通信等の無線あるいは接続ケーブルなどの有線によって接続されてもよい。遠距離通信部１３０は、無線によって無線基地局３と接続し、広域ネットワーク１９に接続される。

【００２２】記憶部１４０は、自身に設定される識別子１１を記憶する。この識別子は、無線通信装置１に予め設定される。例えば、この識別子は、ＩＰアドレス、ＭＡＣアドレス（物理アドレス）等である。また、記憶部１４０は、制御部１６０からの指示に応じて、各種データを記憶する。

【００２３】鍵生成部１５０は、共通鍵生成部１５１を有する。共通鍵生成部１５１は、識別子１１と近距離通信回線１０を介して送信される通信を行う相手側の無線通信装置（例えば、無線通信装置２）に設定される識別符号（例えば、識別子１２）とに基づいて、共通鍵３０を生成する。この共通鍵３０は、識別子１１と識別子１２とに基づいて、一意に算出される値である。

【００２４】また、鍵生成部１５０は、共通鍵生成部１５１によって生成される共通鍵３０と無線基地局（例えば、無線基地局３）から設定される識別符号（例えば、識別符号１７）とに基づいて、秘密鍵と公開鍵（秘密鍵２０と公開鍵２１）とを生成する。この識別符号は、例えば、ＩＰアドレスであり、無線基地局から設定される。

【００２５】制御部１６０は、鍵生成部１５０によって生成される公開鍵を近距離通信部１１０によって相手側



の無線通信装置に送信するとともに、相手側の無線通信装置によって生成された公開鍵を相手側の無線通信装置から近距離通信部１１０によって受信して、通信相手として登録する制御を行う。また、制御部１６０は、鍵生成部１５０によって生成される公開鍵（例えば、公開鍵２１）を用いて、遠距離通信部１３０によって広域ネットワーク１９と接続し、通信を行う制御をする。また、制御部１６０は、共通鍵生成部１５１によって生成される共通鍵（例えば、共通鍵３０）を用いて、信頼関係が確立（詳細は後述する）された無線通信装置に対し、近距離通信部１１０によって通信を行う。

【００２６】なお、図１における無線通信装置２は、無線通信装置１における記憶部１４０に自身に設定される識別子１２を記憶している以外において、無線通信装置１と同様の構成を有する。

【００２７】次に、図１における認証管理サーバ５について図３を用いてさらに詳細に説明する。図３は、認証管理サーバ５の構成を示す概略ブロック図である。この図において、認証管理サーバ５は、通信部５－１と、記憶部５－２と、制御部５－３によって構成される。通信部５－１は、広域ネットワーク１９と無線基地局を介して無線通信装置と通信を行う。

【００２８】記憶部５－２は、図５に示すように、無線通信装置から送信される固有情報（公開鍵）と識別符号との対応関係と、通信相手として信頼関係の確立がなされた無線通信装置同士の対応関係とを認証データとして記憶する。制御部５－３は、記憶部５－２に記憶されている認証データに基づいて、無線通信装置から送信される送信先を示す公開鍵に対応する識別符号を読み出し、読み出した識別符号を通信要求を行った無線通信装置に送信する制御を行う。

【００２９】次に、図２の構成における無線通信装置と図３の構成における認証管理サーバを適用した通信システムの動作について、図２、図３、図４、図５を用いて説明する。ここでは、無線通信装置１と無線通信装置２とが信頼関係の確立を行った後に、遠距離通信回線（第２の通信回線）を用いて通信を行う場合について説明する。また、識別子１１が予め無線通信装置１に設定され、無線通信装置１の記憶部１４０に記憶されており、識別子１２が予め無線通信装置２に設定され、無線通信装置２の記憶部１４０に記憶されているものとする。

【００３０】まず、無線通信装置１を携帯した使用者と無線通信装置２を携帯した使用者とが近距離通信回線１０によって通信可能な距離内に近づき、近距離通信部１１０によって相互に接続する。次に、無線通信装置１は、近距離通信部１１０によって識別子１１を無線通信装置２に送信し、無線通信装置２から送信される識別子１２を受信する。次いで、無線通信装置１は、識別子１１と無線通信装置２から受信した識別子１２とに基づき、共通鍵生成部１５１によって共通鍵３０を生成す

る。さらに、無線通信装置１は、遠距離通信部１３０によって無線基地局３に接続し、識別符号の発行要求を行い、無線基地局３から発行される識別符号１７を受信し、記憶部１４０に記憶する。そして、無線通信装置１は、共通鍵３０と識別符号１７とに基づき、鍵生成部１５０によって公開鍵２１とこの公開鍵２１に対応する秘密鍵２０とを生成し、記憶部１４０に記憶する。

【００３１】一方、無線通信装置２は、無線通信装置１と同様に、近距離通信部１１０によって識別子１１を無線通信装置２に送信すると、無線通信装置１から送信される識別子１２と識別子１１とに基づき、共通鍵生成部１５１によって共通鍵３０を生成する。次いで、無線通信装置２は、遠距離通信部１３０によって無線基地局４に接続し、識別符号の発行要求を行い、無線基地局３から発行される識別符号１８を受信し、記憶部１４０に記憶する。そして、無線通信装置２は、共通鍵３０と識別符号１８とに基づき、鍵生成部１５０によって公開鍵２３とこの公開鍵２３に対応する秘密鍵２２とを生成し、記憶部１４０に記憶する。

【００３２】次に、無線通信装置１は、遠距離通信部１３０によって認証管理サーバ５に公開鍵２１と無線通信装置１の利用者に関する情報とを送信し、認証管理サーバ５によって発行される電子署名が付与された公開鍵２１を受信して記憶部１４０に記憶する。一方、無線通信装置２も同様に、認証管理サーバ５から発行される電子署名が付与された公開鍵２３が記憶される。

【００３３】上述の処理がなされた後、無線通信装置１の制御部１６０は、近距離通信部１１０によって電子署名が付与された公開鍵２１を無線通信装置２に送信し、無線通信装置２から送信される電子署名が付与された公開鍵２３を受信して記憶部１４０に記憶する。これにより、無線通信装置１において、公開鍵２３が、公開鍵に付与された電子署名により、正当性が確認される。また、無線通信装置２において、公開鍵２１が、公開鍵に付与された電子署名により、正当性が確認される。

【００３４】一方、認証管理サーバ５は、無線通信装置１に対して電子署名が付与された公開鍵２１を発行する場合に、電子署名が付与された公開鍵２１と無線通信装置１の識別符号１７とを対応づけて記憶部５－２に認証データとして記憶するとともに、無線通信装置２に対して電子署名が付与された公開鍵２３を発行する場合に、電子署名が付与された公開鍵２３と無線通信装置２の識別符号１８とを対応づけて認証データとして記憶部５－２に記憶する。このとき、記憶部５－２には、例えば、図５に示すような認証データが記憶される。

【００３５】上述の処理が完了することにより、無線通信装置１と無線通信装置２との間において信頼関係の確立が行われる。

【００３６】次に、信頼関係の確立が完了した後、無線通信装置１と無線通信装置２とが近距離通信回線１０によって通信できない遠隔地において通信する場合について説明する。まず、無線通信装置１は、通信を行いたい相手側として、無線通信装置２の電子署名が付与された公開鍵２３（以下、単に「公開鍵２３」と称す）を指定して無線基地局３と広域ネットワーク１９とを介して認証管理サーバ５に呼び出し要求を送信する。管理サーバ５は、無線通信装置１から送信された呼び出し要求先となる公開鍵２３に対応する識別符号１８を記憶部５－２から読み出して、読み出した識別符号１８を広域ネットワーク１９と無線基地局３を介して、無線通信装置１に送信する。

【００３７】無線通信装置１は、認証管理サーバ５から受信した識別符号１８を通信相手先として通信データに設定し、遠距離通信部１３０によって無線基地局３と広域ネットワーク１９とを介して送信する。これにより、無線通信装置１から無線通信装置２に対して通信データが送信される。無線通信装置２についても同様に、上述した同様の手順に従い、無線通信装置１に対して通信データを送信することが可能である。

【００３８】次に、無線基地局４から無線通信装置２に新たな識別符号１８が発行される場合について説明する。無線通信装置２は、移動または通信の開始する場合に、新たな識別符号の発行要求を無線基地局４に行い、無線基地局４から発行される新たな識別符号１８を受信し、記憶部１４０に記憶する。次いで、無線通信装置２は、新たな識別符号１８を秘密鍵２２によって電子署名し、公開鍵２３とともに無線基地局４と広域ネットワーク１９を介して認証管理サーバ５に送信して更新依頼をする。

【００３９】認証管理サーバ５は、無線通信装置２から電子署名された新たな識別符号１８と公開鍵２３とを受信すると、電子署名された新たな識別符号１８を確認した後、公開鍵２３に対応する識別符号として記憶部５－２に記憶して更新する。これにより、以後、無線通信装置１から無線通信装置２に対する送信要求があった場合に、認証管理サーバ５から新たな識別符号１８が無線通信装置１に送信されるので、識別符号１８が更新されても、無線通信装置１と無線通信装置２とが通信を行うことができる。

【００４０】以上説明した実施形態によれば、近距離通信回線１０を介して公開鍵（公開鍵２１、公開鍵２３）を送受信するようにしたので、通信相手を視覚的に確認した相手だけが通信相手の公開鍵（公開鍵２１または公開鍵２３）を知り得ることができ、これにより、他の無線通信装置と識別することが可能である。また、無線通信装置１の利用者および無線通信装置２の利用者が互いに相手を視認した後に信頼関係の確立を行うことができる。

【００４１】次に、上述の方法によって確立した信頼関係の失効について説明する。ここでは、無線通信装置１

と無線通信装置２との間において信頼関係の確立がなされている場合について説明する。無線通信装置１は、無線通信装置２に対する信頼関係が確立した関係を失効する要求である信頼関係失効要求を認証管理サーバ５に送信する。認証管理サーバ５は、無線通信装置１から無線通信装置２に対する信頼関係失効要求を受信すると、記憶部５－２に記憶された認証データから無線端末２の関係（識別符号１８および公開鍵２３）を削除し、広域ネットワーク１９と無線基地局４とを介して無線通信装置２に公開鍵２３の失効を送信する。

【００４２】無線通信装置２は、認証管理サーバ５から公開鍵２３の失効を受信すると、無線通信装置１に対応する秘密鍵２２、共通鍵３０を消去する。一方、無線通信装置１は、無線端末２に対応する公開鍵２３、秘密鍵２０、共通鍵３０を記憶部１４０から消去する。このように、相互に信頼関係の確立を行った無線通信装置のいずれかの無線通信装置から認証管理サーバ５に信頼関係失効要求がなされることにより、確立された信頼関係が無効となる。

【００４３】次に、第２の実施形態について説明する。この実施形態においては、イントラネットを移動体に拡張する場合について図２、図３、図６、図７を用いて説明する。図６において、無線通信装置１および無線通信装置２は、予め近距離通信回線１０を用いて相互に自身に設定された識別子を送信し、上述した手順に従って相互に信頼関係の確立を行う。これにより、無線通信装置１において生成された公開鍵Ｕ１が無線通信装置２に通知され、無線通信装置２において生成された公開鍵Ｕ２が無線通信装置１に通知される。さらに、公開鍵Ｕ１、Ｕ２に対応する秘密鍵Ｒ１、Ｒ２はそれぞれ無線通信装置１、無線通信装置２内に記憶されている。

【００４４】次に、無線通信装置２は、近距離通信回線１０および遠距離通信回線とは別の通信回線６０（イーサネット（登録商標）などのローカル・エリア・ネットワーク）を介してイントラネットＬ１に接続された他の装置（例えばサーバ、コンピュータ、プリンタなど）と通信可能に接続される。そして、無線通信装置２は、イントラネットを介して通信可能な機器のリストである機器リストＫ２（図７）を生成する。

【００４５】一方、無線通信装置１は、近距離通信回線１０のサービス圏外（通信可能な領域外）に移動した後、近距離通信部１１０によって（無線通信装置２に対する同じ通信回線でも別でもよい）を介して入出力端末Ｄ５に接続される。そして、無線通信装置１は、無線通信装置２に接続されているイントラネットＬ１上の機器に対して通信を行う指示が入出力端末Ｄ５から送信されると、無線基地局４、広域ネットワーク１９と無線基地局４とを介して無線通信装置２から機器リストＫ２を取得する。これにより、入出力端末Ｄ５は、無線通信装置１にアクセスすることにより、無線通信装置２に接続されている機器リストＫ２の紹介を行うことが可能となる。



【００４６】次に、入出力端末Ｄ５は、使用者からの指示に応じて、機器リストＫ２の中から通信を行いたい相手側入出力機器を無線通信装置１に指示する。無線通信装置１は、無線通信装置２を介して、入出力端末Ｄ５から指示された相手側入出力機器と通信を確立し、入出力端末Ｄ５からの指示に応じて、相手側入出力機器とデータの送受信を行う。この場合、無線通信装置１は、無線通信装置２に送信するデータを公開鍵暗号手順（公開鍵Ｕ２を用いて暗号化してデータを送信する手順）を用いることにより、経路Ｗ３、無線基地局６、Ｗ４、Ｗ２間は、通信の傍受、改ざんに対して安全に通信を行うことが可能である。

【００４７】次に、第３の実施形態の説明をする。この実施形態においては、信頼関係が確立されていない無線通信装置同士が、お互いに信頼関係の確立をしている機器を媒体として、信頼を確立するよう場合について図８を用いて説明する。この図において、無線通信装置１および無線通信装置２は、信頼関係を確立しており、無線通信装置１および無線通信装置Ｄ３は信頼関係を確立しているものとする。この状況下において、近距離通信回線１０を用いた相互認証を行うことなく無線通信装置２と無線通信装置Ｄ３とが信頼関係を確立して、相互に通信を可能とする場合について説明する。

【００４８】まず、無線通信装置２は、無線基地局Ｄ１２を介して認証管理サーバ５に無線通信装置Ｄ３と共有可能な共通鍵Ｋａを生成するために必要な無線通信装置Ｄ３の識別情報の取得を依頼する。認証管理サーバ５は、認証データに基づいて、無線通信装置２と信頼関係を確立している無線通信装置群の中から無線通信装置Ｄ３と信頼関係の確立がなされている機器として無線通信装置１を検出する（この実施形態では無線通信装置１のみであるが、他に複数ある場合には、その中から適当にひとつを検出する）。

【００４９】次に、認証管理サーバ５は、無線通信装置２に対し、無線通信装置２の識別符号を無線通信装置１に送信するべき指示を出す。次いで、この指示に応じて無線通信装置２から送信される無線通信装置２の識別符号を、記憶部５－２に記憶された無線通信装置１の公開鍵を用いて暗号化して無線通信装置１に送信するとともに、無線通信装置１に対し、受信した無線通信装置２の識別符号を無線通信装置Ｄ３に送信するべき指示を出す。

【００５０】そして、この指示に応じて無線通信装置１から送信される無線通信装置２の識別符号を無線通信装置Ｄ３の公開鍵によって暗号化して無線通信装置Ｄ３に送信するとともに、無線通信装置Ｄ３に対し、無線通信装置Ｄ３の識別符号を無線通信装置１に送信する指示を出す。

【００５１】そして、この指示に応じて無線通信装置３から送信される無線通信装置Ｄ３の識別符号を無線通信装置１の公開鍵によって暗号化して無線通信装置１に送信するとともに、無線通信装置１に対し、無線通信装置Ｄ３の識別符号を無線通信装置２に送信する指示を出す。

【００５２】そして、この指示に応じて無線通信装置１から送信される無線通信装置Ｄ３の識別符号を無線通信装置２の公開鍵によって暗号化して無線通信装置２に送信する。

【００５３】上述のようにして、無線通信装置２と無線通信装置Ｄ３との間において、識別符号交換を遠距離通信回線を用いて間接的に行うことにより、近距離通信回線１０を用いることなく、無線通信装置２と無線通信装置Ｄ３との間における信頼関係を確立することができる。以降の手順は、上述した実施形態と同様に行われる。この実施形態によれば、信頼を確立していない機器同士が、お互いに信頼を確立している機器を媒体として、信頼を確立するようにしたので、近距離通信回線１０を使用できる領域内に接近することなく、信頼関係を確立することができる。

【００５４】以上説明した実施形態によれば、万が一、識別符号（ＩＰアドレス）自体が単体で漏洩した場合においても、そのＩＰアドレスが誰のものかは把握できないので、特定の相手を対象としてＩＰアドレスが悪用される危険性を低減させることができる。

【００５５】なお、上述した実施形態では、第１の通信回線としてＢＬＵＥＴＯＯＴＨを適用した場合について説明したが、ＢＬＵＥＴＯＯＴＨを電話回線に換えて、信頼関係の確立を行うようにしてもよい。これにより、無線通信装置１の利用者と無線通信装置２の利用者とが視認できる距離に近づくことなく、また、共通の信頼関係を確立した無線通信装置を介することなく、信頼関係の確立を行うことが可能である。この場合、無線通信装置の利用者が、予めお互いに会っておく、または、電話を介して相手の確認をする等、確認作業をしておくことによって、通信相手を把握することができ、信頼性を向上させることができる。

【００５６】また、上述した実施形態における無線通信装置と端末（例えば、端末１－ｎ、端末２－ｎ、入出力端末Ｄ５）とを同一筐体内に設けるようにしてもよい。これにより、無線通信装置と端末とを別々に製造する場合に比べて製造コストを低減させて、各種データを送受信することができる効果が得られる。

【００５７】また、上述した実施形態において、電子署名付の公開鍵を交換することにより、無線通信装置１と無線通信装置２との間において信頼関係の確立を行うようにしたが、電子署名が付与されていない状態の公開鍵を相互に交換して信頼関係の確立を行うようにしてもよい。



【００５８】また、上述した共通鍵３０を生成する場合に、識別子１１、識別子１２として識別符号１７、識別符号１８を用いるようにしてもよい。また、通信回線を２経路以上使用して、相手側となる無線通信装置の登録や、データの送受信を行うようにしてもよい。

【００５９】また、図１における無線通信装置１（２、３）、認証管理サーバ５の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより通信を行ってもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。また、「コンピュータシステム」は、ＷＷＷシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フロッピー（登録商標）ディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持しているものも含むものとする。また上記プログラムは、前述した機能の一部を実現するためのものであっても良く、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるものであっても良い。

【００６０】以上、この発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【００６１】

【発明の効果】以上説明したように、この発明によれば、第１の通信回線を用いて通信相手となる無線通信装置の登録に関する通信を行い、第１の通信手段によって登録された通信相手に対し、第１の通信回線と異なる通信回線を用いて通信を行う第２の通信手段とを設けたので、識別符号を第３者に知られないように通信相手に通知することができる効果が得られる。

【００６２】また、この発明によれば、近距離において通信を行う相手側となる無線通信装置の登録を行うようにしたので、無線通信装置の利用者が互いに相手を視認した後に信頼関係の確立を行うことができ、これにより、利用者同士が通信相手を把握した上で通信を行うことができる効果が得られる。

【００６３】また、この発明によれば、信頼を確立していない機器同士が、お互いに信頼を確立している機器を

15

媒体として、信頼を確立するようにしたので、無線通信装置の利用者同士が接近することなく、信頼関係を確立することができる。

【００６４】また、この発明によれば、第１の通信回線を介して識別子を送信しておき、第２の通信回線を介して固有情報によって通信する相手側を指定するようにしたので、識別符号自体が単体で漏洩した場合には、そのＩＰアドレスが誰のものかは把握できないので、特定の相手を対象としてＩＰアドレスが悪用される危険性を低減させることができる。

【図面の簡単な説明】

【図１】　この発明の一実施形態による無線通信装置、認証サーバを適用した通信システムの構成を示す概略ブロック図である。

【図２】　無線通信装置１の構成を示す概略ブロック図である。

【図３】　認証管理サーバ５の構成を示す概略ブロック図である。

【図４】　図１の構成における通信システムの動作を説明するための図面である。

【図５】　認証管理サーバ５の記憶部５－２に記憶される認証データを示す図面である。

【図６】　他の実施形態における通信システムの動作を説明するための図面である。

【図７】　機器リストＫ２の一例を示す図面である。

16

【図８】　他の実施形態における通信システムの動作を説明するための図面である。

【符号の説明】

１、２、Ｄ３　無線通信装置　　３、４　無線基地局

５　認証管理サーバ　　５－１　通信部

５－２　記憶部　　５－３　制御部

１０　近距離通信回線　　１１、１２　識別子

１３、１４、１５、１６　通信回線

１７、１８　識別符号　　１９　広域ネットワーク

２０、２２　秘密鍵　　２１、２３　公開鍵

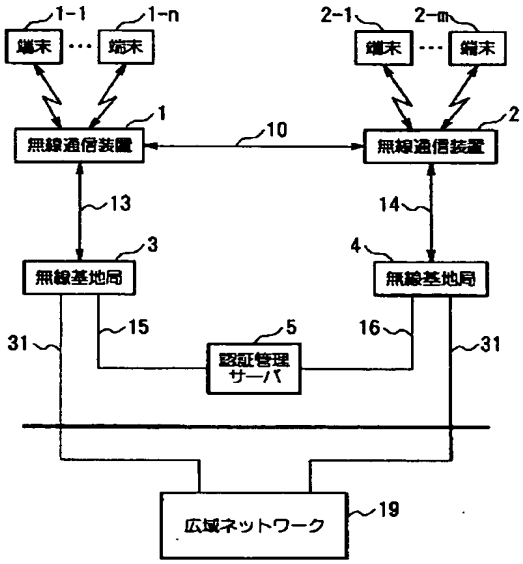
３０　共通鍵　　１００　通信部

１１０　近距離通信部　　１３０　遠距離通信部

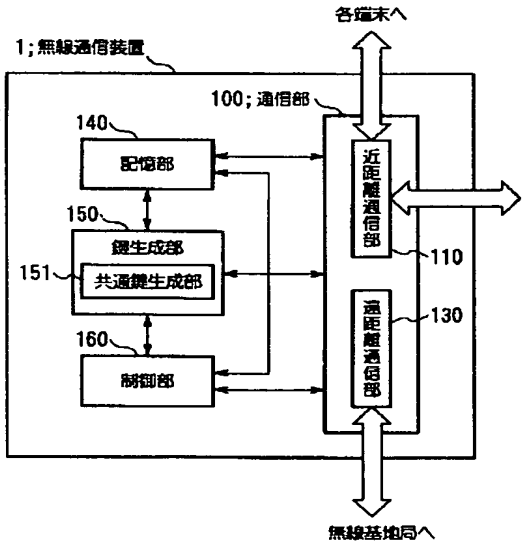
１４０　記憶部　　１５０　鍵生成部

１５１　共通鍵生成部　　１６０　制御部

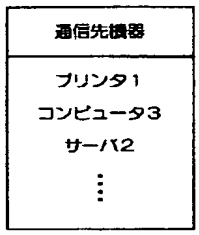
【図１】



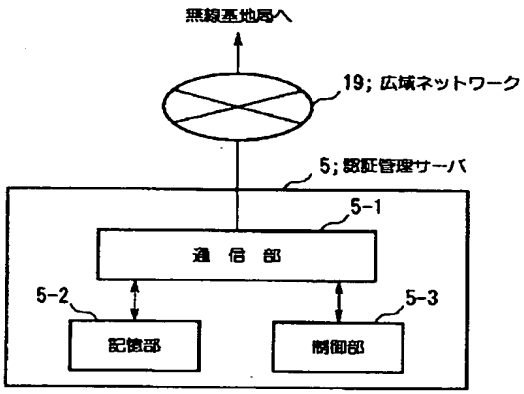

【図２】



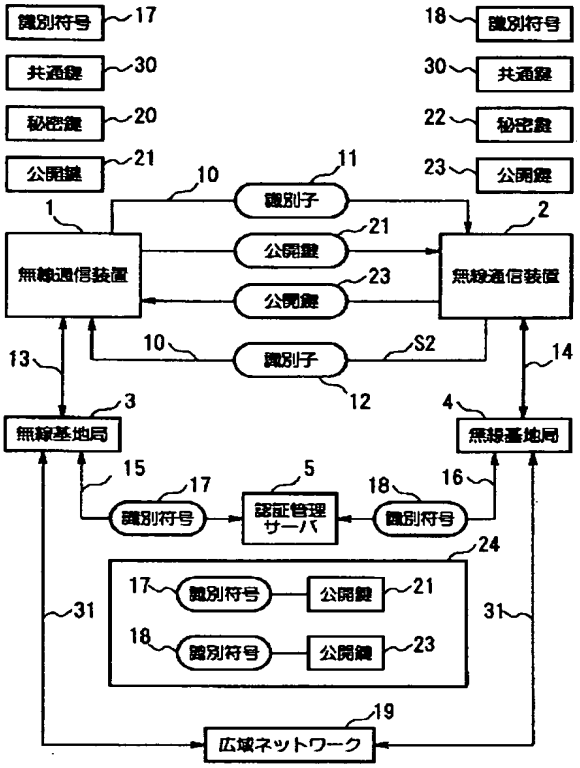

【図７】



【図３】



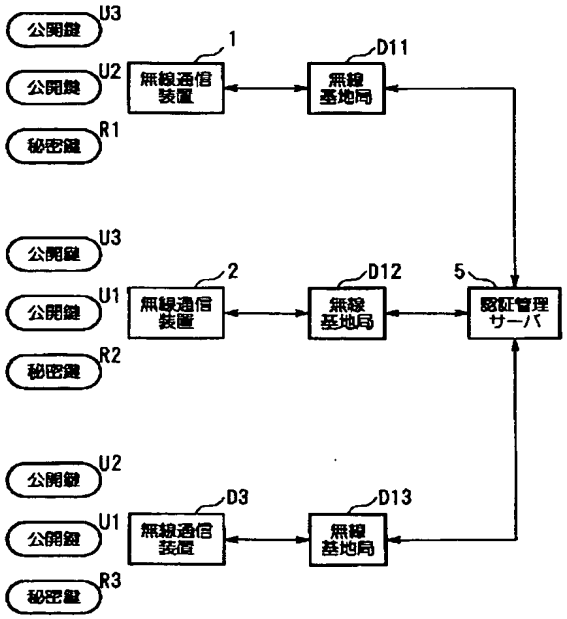

【図４】



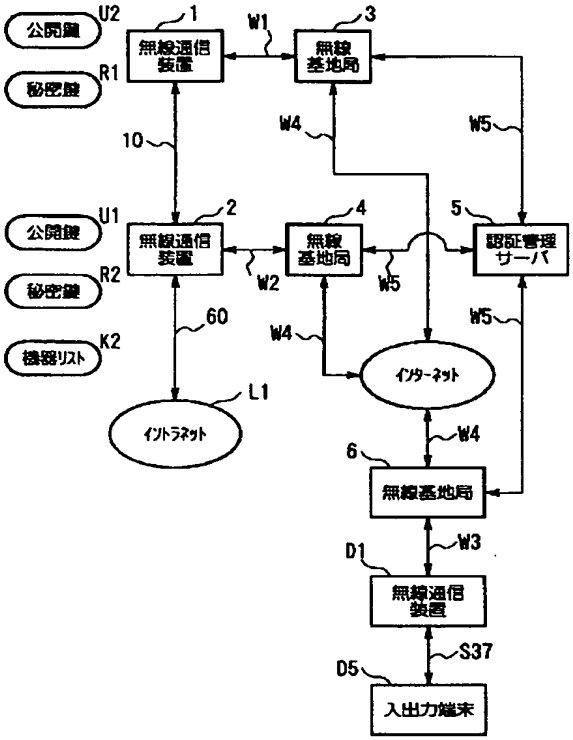

【図５】

| 識別符号 | 公開鍵 | 信頼関係の確立 |
|---|---|---|
| 識別符号１７ | 公開鍵２１ | 無線通信装置２ |
| 識別符号１８ | 公開鍵２３ | 無線通信装置１ |
| ⋮ | ⋮ | |

【図８】



【図６】


公開鍵
U2
1
無線通信装置
W1
3
無線基地局
秘密鍵
R1
10
W4
W5
公開鍵
U1
2
無線通信装置
4
無線基地局
5
認証管理サーバ
秘密鍵
R2
W2
W5
60
W4
W5
機器リスト
K2
インターネット
L1
イントラネット
W4
6
無線基地局
W3
D1
無線通信装置
S37
D5
入出力端末